BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	103 02 456.5
Anmeldetag:	23. Januar 2003
Anmelder/Inhaber:	ROBERT BOSCH GMBH, Stuttgart/DE
Bezeichnung:	Vorrichtung für sicherheitskritische Anwendungen und sichere Elektronik-Architektur
IPC:	G 06 F 11/00

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 5. Dezember 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Ebert

A 9161
06/00
EDV-L

EV 321 891 805 US

R. 303913
16.12.2002 SB/koc
ROBERT BOSCH GMBH, 70442 STUTTGART

BESCHREIBUNG

Vorrichtung für sicherheitskritische Anwendungen und sichere Elektronik-Architektur

STAND DER TECHNIK

Die vorliegende Erfindung betrifft eine sichere Elektronik-Architektur, und betrifft insbesondere eine Rechnervorrichtung für sicherheitskritische Anwendungen, bei der eine Speichereinheit und mindestens eine Prozessoreinheit chipflächeneffizient und kosteneffizient zusammenwirken.

Verteilte, sicherheitsrelevante Systeme werden beispielsweise in dem Fahrzeugbereich bzw. in der Fahrzeugtechnik als X-by-wire-Systeme eingesetzt, wobei die funktionale Sicherheit derartiger Systeme zu gewährleisten ist. Ein bekanntes Steuergerät zur Steuerung sicherheitskritischer Anwendungen ist in der DE 199 02 031 A1 beschrieben. Bekannt sind bei Einrechner-Steuergeräten Verfahren mit Selbsttest, Plausibilitätsüberwachung und sogenanntem Watch-dog.

In der DE 199 02 031 A1 ist offenbart, dass eine Überwachungseinheit erste Mittel zur Messung des Ruhestroms des Mikrocomputers aufweist und dass weiterhin zweite Mittel vorgesehen sind, um den Mikrocomputer mit einem Testdatensignal zu beaufschlagen, um das Testdatensignal zu verarbeiten und ein Testdatenausgangssignal des Mikrocomputers mit einem entsprechenden Testdatenausgangssignal der Überwachungseinheit zu vergleichen.

Ein weiteres bekanntes Mikroprozessorsystem für sicherheitskritische Regelungen ist in der DE 195 29 434 A1 beschrieben, wobei zugeführte Daten redundant verarbeitet werden, indem Zentraleinheiten bzw. CPUs über separate Bussysteme an die

Festwert- und an die Schreib-Lese-Speicher sowie an Eingabe- und Ausgabeeinheiten angeschlossen sind und die Bussysteme untereinander durch Treiberstufen verbunden sind.

Vollständige Rechnervorrichtungen umfassen üblicherweise Speichereinheiten zur Speicherung von Prozessdaten, Prozessoreinheiten zur Verarbeitung von Prozessdaten und eine Specherverwaltungseinheit zur Steuerung von Speicherzugriffen. Weiterhin werden Fehlererfassungseinheiten eingesetzt, um Fehler in Speichereinheiten zu erfassen und um diese dann gegebenenfalls unter Zuhilfenahme von Fehlerkorrektureinheiten zu korrigieren. Im Allgemeinen ist jeder Speichereinheit eine Fehlererfassungseinheit bzw. eine Fehlerkorrektureinheit zugeordnet. Für die Überprüfung von Prozessoreinheiten, welche mit den Speichereinheiten wechselwirken, ist im Allgemeinen eine Selbsttesteinheit vorgesehen, welche einer entsprechenden Prozessoreinheit zugeordnet ist. Herkömmlicherweise ist die Speichereinheit zusammen mit einer zugeordneten Prozessoreinheit auf einer Chipfläche bzw. einem Chip angeordnet. Hierbei weist die Speichereinheit einen wesentlich höheren Flächenbedarf als die Prozessoreinheit auf, d.h. der größte Teil der Chipfläche, auf welcher eine Speichereinheit und eine Prozessoreinheit angeordnet sind, wird von der Speichereinheit eingenommen. Beispielsweise beträgt das Flächenverhältnis der Fläche der Speichereinheit zu der Fläche der Prozessoreinheit 30:1.

Weiterhin ist die Wahrscheinlichkeit eines Auftretens von Fehlern auf dem Chip proportional zur Fläche des Chips, was bedeutet, dass die Fehlerwahrscheinlichkeit bezüglich der Speichereinheit wesentlich größer als die Fehlerwahrscheinlichkeit bezüglich des Prozessors ist.

Ein Rechnersystem, das einen Dualkern einsetzt, ist in der DE 195 29 434 A1 beschrieben. Dieses System weist ein sogenanntes "fail-silent"-Verhalten auf, d.h. das System weist ein definiertes Verhalten auf, welches für die Funktionsfähigkeit der

übrigen Schaltungskomponenten unschädlich ist, wenn ein Fehler erkannt wird.

Ein Nachteil des Dualkernkonzepts besteht darin, dass dieser empfindlich gegen Common-mode-Fehler ist, d.h. eine Störung durch kurzzeitige Spitzen auf der Versorgungsspannung oder eine elektromagnetische Störung beeinflusst beide (Rechner-) Kerne in gleicher Weise, so dass Fehler, welche einer Vergleichseinheit zugeführt werden, nicht erkannt werden können.

Damit kann ein nicht erkannter Fehler eine nicht zu erkennende Auswirkung in der Anwendung hervorrufen. Auch bei einer Verwendung des sogenannten "Lockstep-Konzepts" sind Common-mode-Fehler möglich, wenn eine Störung länger andauert als eine Dauer einer Verzögerungszeit zwischen den beiden Kernen. Die Dauer der Verzögerungszeit ist hingegen auf die Zeit einer Befehlsausführung begrenzt, da bei einer längeren Dauer die beiden Kerne unwiederbringlich ihre Synchronität verlieren können. Beispielsweise könnte für die Dauer einer Befehlsausführung ein externes Interrupt-Signal bereitgestellt werden, das den nicht-verzögerten Kern zur Ausführung eines Interrupt-Programms veranlasst, wohingegen der verzögert arbeitende Kern sein normales Programm abarbeitet, weil kein Interrupt-Signal mehr anliegt.

Ein weiterer Nachteil des Dualkernkonzepts besteht darin, dass Fehler erst dann erfasst werden, wenn die entsprechenden Ressourcen benötigt werden, z.B. wenn ein bestimmter Abschnitt des Programms durchlaufen wird oder wenn ein Teil des Kerns benötigt wird, bei dem dann aktuell ein Unterschied zwischen den Ergebnissen der beiden Kerne auftritt.

Die Aufgabe der vorliegenden Erfindung besteht darin, eine Rechnervorrichtung zu schaffen, bei der die Chipflächen bezüglich der bei den auf diesen Chips angeordneten Speicher- und Prozessoreinheiten auftretenden Fehlern besser genutzt werden und bei der eine Speicher-Prozessor-Anordnung optimiert ist.

Diese Aufgabe wird durch eine Rechnervorrichtung mit den Merkmalen des Anspruchs 1 gelöst.

Weiterhin wird die Aufgabe erfindungsgemäß durch ein im Patentanspruch 8 angegebenes Verfahren gelöst.

Weitere Ausgestaltungen der Erfindung ergeben sich aus den Unteransprüchen.

Ein wesentlicher Gedanke der Erfindung besteht darin, Speichereinheiten zusammen mit Fehlererfassungseinheiten und/oder Fehlerkorrektureinheiten und gleichzeitig Prozessoreinheiten zusammen mit zugeordneten Selbsttesteinheiten auf einem gemeinsamen Chip anzuordnen, wobei einer Kombination aus Speichereinheit und Fehlererfassungseinheit bzw. Fehlerkorrektureinheit mehr als eine Kombination aus einer Prozessoreinheit - auch als Prozessorsystem bezeichnet - und einer zugeordneten Selbsttesteinheit zugeordnet ist.

Die erfindungsgemäße Rechnervorrichtung weist dann den wesentlichen Vorteil auf, dass eine Kombination von einem sich selbst überwachenden (Selbsttest) -Rechnerkern (core mit BIST (built in self test)-Konzept) und einer fehlersicheren Speichereinheit bereitgestellt wird. In vorteilhafter Weise vermeidet das Einzelkern-BIST-Konzept die Nachteile eines Dualkern-Konzepts, da durch eine Kombination einer Speichereinheit, welche eine zugeordnete Fehlererfassungseinheit und/oder eine zugeordnete Fehlerkorrektureinheit aufweist, mit einer Prozessoreinheit, welche eine Selbsttesteinheit zugeordnet aufweist, Fehlertoleranzlevel erzielt werden, welche für den Kern "fail-silent", für die Speichereinheit mit zugeordneter Fehlererfassungseinheit "fail-silent" und für die Speichereinheit mit zugeordneter Fehlerkorrektureinheit "fail-operational" bezüglich des Erstfehlers und „fail-silent" bezüglich des Zweitfehlers sind. Dies bedeutet, dass der Kern einen Fehler entdecken kann und sich dann passiv auf ein defi-

niertes, für die übrigen Schaltungseinheiten unschädliches Verhalten schaltet. Der Speicher mit Fehlererfassungseinheit weist das gleiche Verhalten auf, wohingegen der Speicher mit Fehlerkorrektureinheit für den ersten auftretenden Fehler ohne Einschränkungen weiterarbeitet und für den zweiten auftretenden Fehler ein definiertes, unschädliches Verhalten aufweist.

Die erfindungsgemäße Rechnervorrichtung für sicherheitskritische Anwendungen weist im Wesentlichen auf:

a) mindestens eine Prozessoreinheit;

b) eine Speichereinheit zur Speicherung von Prozessdaten;

c) eine Speicherverwaltungseinheit zur Steuerung von Speicherzugriffen in der Rechnervorrichtung;

d) eine Fehlererfassungseinheit zur Erfassung von Fehlern in der Speichereinheit; und

e) mindestens eine der Prozessoreinheit zugeordneten Selbsttesteinheit,

wobei die Rechnervorrichtung weiter Verbindungsmittel zur Verbindung der Prozessoreinheiten untereinander und mit der Speicherverwaltungseinheit umfasst, wobei die Prozessoreinheiten zusammen mit der Speichereinheit auf einer gemeinsamen Chipfläche angeordnet sind.

In den Unteransprüchen finden sich vorteilhafte Weiterbildungen und Verbesserungen des jeweiligen Gegenstandes der Erfindung.

Gemäß einer bevorzugten Weiterbildung der vorliegenden Erfindung ist die Fehlererfassungseinheit als eine Fehlerkorrektureinheit ausgebildet, so dass in vorteilhafter Weise eine Kor-

rektur von Fehlern in der Speichereinheit bereitgestellt werden kann.

Gemäß einer weiteren bevorzugten Weiterbildung der vorliegenden Erfindung ist jeder Prozessoreinheit jeweils eine Selbsttesteinheit zur Durchführung eines Selbsttests zugeordnet.

Gemäß einer weiteren bevorzugten Weiterbildung der vorliegenden Erfindung weist die Rechnervorrichtung zwei durch Verbindungsmittel gekoppelte Prozessoreinheiten auf, welchen jeweils eine Selbsttesteinheit zugeordnet ist.

Gemäß noch einer weiteren bevorzugten Weiterbildung der vorliegenden Erfindung ist eine Kombination von Rechnervorrichtungen, die eine gleiche oder unterschiedliche Anzahl von Prozessoreinheiten aufweisen, mittels mindestens einer Verbindungseinheit bereitgestellt. Hierbei sind die Verbindungsmittel zweckmäßigerweise derart gestaltet, dass eine entsprechende Bitanzahl auf den Verbindungsmitteln übertragen werden kann.

Gemäß noch einer weiteren bevorzugten Weiterbildung der vorliegenden Erfindung ist der Rechnervorrichtung jeder Speichereinheit jeweils eine Fehlerkorrektureinheit zugeordnet.

Gemäß noch einer weiteren bevorzugten Weiterbildung der vorliegenden Erfindung sind die Speicherverwaltungseinheit zur Steuerung von Speicherzugriffen in der Rechnervorrichtung und die mindestens eine Prozessoreinheit als eine einzige Einheit integral ausgebildet.

Weiterhin weist das erfindungsgemäße Verfahren zur Prozessdatenverarbeitung in einer Rechnervorrichtung für sicherheitskritische Anwendungen im Wesentlichen die folgenden Schritte auf:

a) Verarbeiten von Prozessdaten in mindestens einer Prozessoreinheit, wobei

a1) die mindestens eine Prozessoreinheit mittels mindestens einer der Prozessoreinheit zugeordneten Selbsttesteinheit getestet wird; und

a2) in der Rechnervorrichtung die Prozessoreinheiten untereinander und mit der Speicherverwaltungseinheit mittels Verbindungsmitteln verbunden sind, wobei die Prozessoreinheiten zusammen mit der Speichereinheit auf einer gemeinsamen Chipfläche angeordnet sind;

b) Steuern von Speicherzugriffen in der Rechnervorrichtung mittels einer Speicherverwaltungseinheit;

c) Speichern von Prozessdaten in einer Speichereinheit; und

d) Erfassen von Fehlern in der Speichereinheit (102) mittels einer Fehlererfassungseinheit.

Gemäß noch einer weiteren bevorzugten Weiterbildung der vorliegenden Erfindung werden mittels einer Fehlerkorrektureinheit Fehler in der Speichereinheit korrigiert.

Gemäß noch einer weiteren bevorzugten Weiterbildung der vorliegenden Erfindung werden in der Rechnervorrichtung zwei durch Verbindungsmittel gekoppelte Prozessoreinheiten jeweils durch zugeordnete Selbsttesteinheiten getestet.

Gemäß noch einer weiteren bevorzugten Weiterbildung der vorliegenden Erfindung werden Rechnervorrichtungen, die eine gleiche oder unterschiedliche Anzahl von Prozessoreinheiten aufweisen, mittels mindestens einer Verbindungseinheit kombiniert.

Gemäß noch einer weiteren bevorzugten Weiterbildung der vorliegenden Erfindung wird die Speichereinheit in der Rechnervorrichtung jeweils mittels einer zugeordneten Fehlerkorrektureinheit auf Fehler überprüft und korrigiert.

Gemäß noch einer weiteren bevorzugten Weiterbildung der vorliegenden Erfindung wird die mindestens eine Prozessoreinheit mittels einer zugeordneten Selbsttesteinheit getestet.

Gemäß noch einer weiteren bevorzugten Weiterbildung der vorliegenden Erfindung gibt die Selbsttesteinheit eine Fehlermeldung über Selbsttesteinheit-Ausgabemittel zu einer externen Anzeigeeinheit und/oder einer Fehlerverarbeitungseinheit aus, wenn eine Prozessoreinheit durch die zugeordnete Selbsttesteinheit als fehlerhaft erkannt wird.

Gemäß noch einer weiteren bevorzugten Weiterbildung der vorliegenden Erfindung tauschen die Prozessoreinheiten Anfangswerte, Zwischenergebnisse bzw. Zwischenwerte und Endergebnisse über die Verbindungsmittel zwischen den Prozessoreinheiten aus und überprüfen dieselben auf Gleichheit.

Gemäß noch einer weiteren bevorzugten Weiterbildung der vorliegenden Erfindung gibt die Prozessoreinheit eine Fehlermeldung über Prozessoreinheit-Ausgabemittel zu einer externen Anzeigeeinheit und/oder einer Fehlerverarbeitungseinheit aus, wenn die Prozessoreinheit eine Abweichung zwischen den Zwischenergebnissen bzw. Zwischenwerten und/oder Endergebnissen feststellt.

Gemäß noch einer weiteren bevorzugten Weiterbildung der vorliegenden Erfindung wird bei einem Auftreten von Fehlern in der Speichereinheit eine Fehlermeldung über Fehlererfassungseinheit-Ausgabemittel zu einer externen Anzeigeeinheit und/oder einer Fehlerverarbeitungseinheit ausgegeben.

Gemäß noch einer weiteren bevorzugten Weiterbildung der vorliegenden Erfindung wird bei einem Auftreten von Fehlern in der Speichereinheit eine Fehlermeldung über die Speicherverwaltungseinheit zu der Prozessoreinheit übertragen, von welcher die Fehlermeldung anschließend über die Prozessoreinheit-Ausgabemittel zu einer externen Anzeigeeinheit und/oder einer Fehlerverarbeitungseinheit ausgegeben wird.

Ausführungsbeispiele der Erfindung sind in den Zeichnungen dargestellt und in der nachfolgenden Beschreibung näher erläutert.

In den Zeichnungen zeigen:

Figur 1 eine erfindungsgemäße Rechnervorrichtung mit einer Speichereinheit mit zugeordneter Fehlererfassungseinheit und einer einzigen Prozessoreinheit mit zugeordneter Selbsttesteinheit;

Figur 2 eine Rechnervorrichtung gemäß einem weiteren bevorzugten Ausführungsbeispiel der vorliegenden Erfindung, wobei die Fehlererfassungseinheit der Figur 1 durch eine Fehlerkorrektureinheit ersetzt ist;

Figur 3 eine Rechnervorrichtung mit zwei Prozessoreinheiten gemäß einem weiteren bevorzugten Ausführungsbeispiel der vorliegenden Erfindung;

Figur 4 die Kombination einer Rechnervorrichtung mit zwei Prozessoreinheiten mit einer weiteren Rechnervorrichtung mit einer Prozessoreinheit gemäß einem weiteren bevorzugten Ausführungsbeispiel der vorliegenden Erfindung; und

Figur 5 die Kombination zweier Rechnervorrichtungen, welche jeweils zwei Prozessoreinheiten gemäß Figur 3 aufwei-

sen, gemäß einem weiteren bevorzugten Ausführungsbeispiel der vorliegenden Erfindung.

In den Figuren bezeichnen gleiche Bezugszeichen gleiche oder funktionsgleiche Komponenten oder Schritte.

In der in Figur 1 gezeigten Rechnervorrichtung 100, welche auf einer einzigen Chipfläche anordenbar ist, steuert eine Speicherverwaltungeinheit (MMU = Memory Management Unit) 103 Speicherzugriffe in der Rechnervorrichtung 100, wobei die Speicherverwaltungseinheit 103 einerseits mit der Prozessoreinheit 104 und andererseits mit der Speichereinheit 102 wechselwirkt. Erfindungsgemäß ist der Speichereinheit 102 eine Fehlererfassungseinheit 101 zugeordnet, mit welcher Fehler in der Speichereinheit 102 erfasst werden.

Wegen der durch die Speichereinheit 102 beanspruchten, größeren Chipfläche kann für die Speichereinheit 102 ein höherer Fehlertoleranzlevel erforderlich sein, als für den Rechnerkern, d.h. die Prozessoreinheit 104. Die von der Speichereinheit eingenommene Chipfläche kann um eine Größenordnung über der von der Prozessoreinheit eingenommenen Chipfläche liegen. Bei einer vereinfachten Betrachtung ist eine Fehlerwahrscheinlichkeit proportional zur eingenommenen Chipfläche. Die Prozessoreinheit 104 wird durch eine Selbsttesteinheit 105, die der Prozessoreinheit 104 zugeordnet ist und mit dieser über Prozessorverbindungsmittel 201, 201a, 201b verbunden ist, überwacht bzw. wird ein Selbsttest der Prozessoreinheit 104 durch die Selbsttesteinheit 105 durchgeführt. Durch das Einzelkern-Konzept, das in Figur 1 schematisch veranschaulicht ist, können die obenstehend geschilderten Nachteile des Dualkern-Konzepts vermieden werden. Hierbei ist der Rechnerkern "fail-silent" ausgeführt, d.h. bei einem Auftreten eines Fehlers geht das Gesamtsystem des Rechnerkerns in einen definierten Zustand über, welcher für die übrigen Schaltungskomponenten unschädlich ist.

Die mit einem höheren Fehlertoleranzlevel versehene Speichereinheit 102 ist entweder "fail-silent" oder "fail-operational" ausgeführt. In Figur 1 ist eine Speichereinheit gezeigt, welche "fail-silent" unter Verwendung der Fehlererfassungseinheit 101 ausgeführt ist. Somit lässt sich ein "fail-silent"-Mikrocomputer sowohl chipflächen-optimal als auch kosten-optimal verwirklichen.

Figur 2 unterscheidet sich von Figur 1 darin, dass die Speichereinheit 102 "fail-operational" ausgelegt ist, d.h. die Fehlererfassungseinheit 101 ist durch eine Fehlerkorrektureinheit 106 ersetzt.

Es sei darauf hingewiesen, dass die Speichereinheit 102 sowohl einen ROM (Read Only Memory = Lesespeicher) als auch einen RAM (Random Access Memory = Schreib/Lese-Speicher) umfassen kann.

In vorteilhafter Weise kann bei einem Flash-ROM sogar in Betrieb eine Information von Speicherzellen der Speichereinheit 102 neu programmiert werden, wodurch eine Korrekturmöglichkeit der Speichereinheit 102 bereitgestellt wird. Somit kann in einer Rechnervorrichtung 100b gemäß Figur 2, welche einen Flash-ROM als eine Speichereinheit 102 zusammen mit einer Fehlerkorrektureinheit 106 enthält, nicht nur die Prozessoreinheit 104 die erhaltenen Daten aus der Speichereinheit vor einer Verarbeitung korrigieren, sondern die Prozessoreinheit kann darüber hinaus auch die Speichereinheit mit dem korrigierten Datenwert neu programmieren. Hierdurch ergeben sich erhebliche Vorteile bezüglich einer Vereinfachung einer sicheren Elektronik-Architektur bzw. einer Rechner-Architektur von Steuergeräten:

(i) Anwendungen mit einer "fail-silent"-Forderung bezüglich eines Mikrocomputers beruhen auf einem 1-fehlertoleranten Speicher mit "fail-silent"-Prozessoreinheit;

(ii) Anwendungen mit einer Anforderung nach einer 1-Fehlertoleranz bezüglich des Mikrocomputers setzen zwei sichere Prozessoreinheiten ein, die je nach den weiteren Anforderungen bezüglich einer Fehlertoleranz der Spannungsversorgung und einer Fehlertoleranz gegenüber Common-mode-Fehlern in einem oder in zwei Steuergeräten untergebracht sein können, wie untenstehend unter Bezugnahme auf Figur 3 erläutert werden wird;

(iii) Anwendungen mit einer Anforderung nach einer 1-Fehlertoleranz bezüglich der Mikrocomputer beruhen auf drei sicheren Prozessoreinheiten, die je nach den weiteren Anforderungen bezüglich einer Fehlertoleranz der Spannungsversorgung und einer Fehlertoleranz gegenüber Common-mode-Fehlern aus einem, zwei oder drei Steuergeräten bestehen können; und

(iv) weitere Kombinationen aus einem "fail-operational"-Modul und einem sicheren Mikrocomputer können bereitgestellt werden.

Die in den Figuren 1 und 2 gezeigten Rechnervorrichtungen können jeweils für zwei unterschiedliche Versorgungsspannungen verdoppelt werden, so dass durch Verdoppelung der Rechnervorrichtung 100b gemäß Figur 2 ein zweikanaliges System aus zwei Rechnervorrichtungen entsteht, das 1-fehlertolerant bezüglich Speicherfehler und ebenfalls 1-fehlertolerant bezüglich Prozessorfehler ist. Durch Verwendung zweier Versorgungsspannungen ist das System auch gegen Fehler der Versorgungsspannungen 1-fehlertolerant. Weiterhin entsteht durch Verdoppelung der Rechnervorrichtung 100b aus Figur 2 ein zweikanaliges System aus zwei Rechnervorrichtungen, das 2-fehlertolerant bezüglich Speicherfehler und 1-fehlertolerant bezüglich Prozessorfehler ist. Durch Verwendung zweier Versorgungsspannungen ist das System wiederum gegen Fehler der Versorgungsspannungen 1-fehlertolerant.

Es sei darauf hingewiesen, dass unter einem 1-fehlertolerantem Speicher oder einem 1-fehlertoleranten Prozessorsystem bzw.

einem 2-fehlertolerantem Speicher oder einem 2-fehlertoleranten Prozessorsystem Speicher- bzw. Prozessorsysteme verstanden werden, die bezüglich des Auftretens eines bzw. zweier Fehler fehlertolerant sind.

So ist es gemäß Figur 2 zwar möglich, dass das Gesamtsystem bei einem Auftreten eines Fehlers in der Speichereinheit 102 weiterarbeitet (1-fehlertoleranter Speicher), wenn hingegen in der Prozessoreinheit 104 ein Fehler auftritt, wird die Bearbeitung abgebrochen und das System fährt in einen definierten Zustand, bzw. weist ein definiertes Verhalten auf, das für die übrigen Schaltungskomponenten unschädlich ist ("fail-silent"-Prozessor).

Figur 3 zeigt eine Rechnervorrichtung 100a, die neben einem 1-fehlertoleranten Speicher (Speichereinheit 102) auch ein 1-fehlertolerantes Prozessorsystem bereitstellt. Zu diesem Zweck sind in der in Figur 3 dargestellten Rechnervorrichtung 100 zwei unabhängige Prozessoreinheiten 104a und 104b bereitgestellt, welche untereinander durch ein erstes Verbindungsmittel 108a verbunden sind, um Prozessdateninformation auszutauschen. Weiterhin sind beide Prozessoreinheiten 104a, 104b mittels eines zweiten Verbindungsmittels 108b mit der Speicherverwaltungseinheit 103 verbunden.

Jeder Prozessoreinheit ist, wie obenstehend unter Bezugnahme auf die Figuren 1 und 2 erläutert, weiterhin eine entsprechende Selbsttesteinheit 105a bzw. 105b zugeordnet, welche in der erläuterten Weise Selbsttests bezüglich der jeweiligen Prozessoreinheit 104a, 104b durchführen. Auf diese Weise ist es durch die erfindungsgemäße Rechnervorrichtung vorteilhaft möglich, einen 1-fehlertoleranten Speicher mit einem 1-fehlertoleranten Prozessorsystem zu verkoppeln. Somit kann in einer der beiden Prozessoreinheiten 104a, 104b ein Fehler auftreten, ohne dass ein Verarbeitungsbetrieb in der gesamten Rechnervorrichtung 100a abgebrochen werden muss.

Die Figuren 4 und 5 sind Beispiele weiterer Kombinationsmöglichkeiten, welche durch die erfindungsgemäße Vorrichtung und das erfindungsgemäße Verfahren zur Prozessdatenverarbeitung in einer Rechnervorrichtung für sicherheitskritische Anwendungen ermöglicht werden.

In Figur 4 ist eine Rechnervorrichtung 100a, welche der unter Bezugnahme auf Figur 3 beschriebenen Rechnervorrichtung entspricht, mit einer Rechnervorrichtung 100b, welche der unter Bezugnahme auf Figur 2 beschriebenen Rechnervorrichtung entspricht, kombiniert. Die Rechnervorrichtungen 100a und 100b sind durch eine Verbindungseinheit 107a untereinander verbunden, wobei die Verbindungseinheit 107a derart ausgelegt ist, dass eine dem gewünschten Fehlertoleranzlevel entsprechende Anzahl von Verbindungsleitungen bereitgestellt wird. Hier sind zwei bidirektionale Verbindungsleitungen vorgesehen, so dass die Verbindungseinheit fehlertolerant für einen Fehler ausgeführt ist. Nach dem Ausfall einer Verbindungsleitung ist die Verbindung noch über die zweite Verbindungsleitung betriebsfähig.

Durch die in Figur 4 gezeigte erfindungsgemäße Kombination ergibt sich eine Anordnung mit drei Rechnerkernen, wodurch das Gesamtsystem aus einem 1-fehlertoleranten Speicher und einem 1-fehlertoleranten Prozessorsystem an zwei Versorgungsspannungen besteht. Es sei darauf hingewiesen, dass hierbei die Versorgungsspannung ebenfalls zwei-kanalig ausgelegt sein muss. Weiterhin ist es möglich - obwohl in der Figur nicht dargestellt -, dass mehr als zwei Rechnerkerne bzw. Prozessoreinheiten 104a, 104b in einer Rechnervorrichtung 100a angeordnet sind. Durch den modularen Aufbau, wie er in den Figuren 4 und 5 gezeigt ist, lassen sich anwendungsspezifische Anforderungen an eine Fehlertoleranz bezüglich der Speichereinheiten und/oder der Prozessoreinheiten einfach erfüllen.

Figur 5 zeigt ein weiteres Ausführungsbeispiel gemäß der vorliegenden Erfindung, wobei hier zwei Rechnervorrichtungen 100a

und 100c über die Verbindungseinheit 107b, welche eine entsprechende Anzahl von Verbindungen (hier: 4) aufweist, die entsprechend der gewünschten Fehlertoleranz für Fehler an den Verbindungsleitungen gewählt wird. Bei der bidirektionalen Ausführung der vier Verbindungsleitungen besteht eine Toleranz gegenüber drei fehlerhaften Verbindungsleitungen.

Die beiden Rechnervorrichtungen 100a und 100c des Ausführungsbeispiels entsprechen jeweils der unter Bezugnahme auf Figur 3 beschriebenen Rechnervorrichtung 100a. Durch die in Figur 5 gezeigte Konfiguration wird ein symmetrisches System gebildet, das aus zwei Rechnervorrichtungen 100a, 100c besteht, die an zwei Versorgungsspannungen angeschlossen sind und jeweils eine 1-fehlertolerante Speichereinheit 102 und ein 1-fehlertolerantens Prozessorsystem enthalten. Das Gesamtsystem nach Figur 5 ist dann 2-fehlertolerant gegen Speicherfehler in den Speichereinheiten 102 und 3-fehlertolerant gegen Fehler in den Prozessoreinheiten 104a, 104b.

Es sei darauf hingewiesen, dass die Versorgungsspannungen hier ebenfalls zweikanalig ausgelegt sein müssen.

Mit der erfindungsgemäßen Anordnung und dem erfindungsgenmäßen Verfahren wird es ermöglicht, dass die Selbsttesteinheit 105; 105a, 105b eine Fehlermeldung über Selbsttesteinheit-Ausgabemittel 202, 202a, 202b zu einer externen Anzeigeeinheit und/oder einer Fehlerverarbeitungseinheit ausgibt, wenn eine Prozessoreinheit 104, 104a, 104b durch die zugeordnete Selbsttesteinheit 105; 105a, 105b als fehlerhaft erkannt wird. Weiterhin ist es zweckmäßig, dass die Prozessoreinheiten 104, 104a, 104b Anfangswerte, Zwischenwerte bzw. Zwischenergebnisse und Endergebnisse über die Verbindungsmittel 108a, 108b zwischen den Prozessoreinheiten 104, 104a, 104b austauschen und auf Gleichheit überprüfen.

In vorteilhafter Weise ist sichergestellt, die Prozessoreinheit 104, 104a, 104b eine Fehlermeldung über Prozessoreinheit-

Ausgabemittel 203, 203a, 203b zu einer externen Anzeigeeinheit und/oder einer Fehlerverarbeitungseinheit ausgibt, wenn die Prozessoreinheit 104, 104a, 104b eine Abweichung zwischen den Zwischenergebnissen und/oder Endergebnissen feststellt. Darüber hinaus ist es möglich, dass bei einem Auftreten von Fehlern in der Speichereinheit 102 eine Fehlermeldung über Fehlererfassungseinheit-Ausgabemittel 204 zu einer externen Anzeigeeinheit und/oder einer Fehlerverarbeitungseinheit ausgegeben wird. Andererseits ist es ebenfalls sichergestellt, dass bei einem Auftreten von Fehlern in der Speichereinheit 102 eine Fehlermeldung über die Speicherverwaltungseinheit 103 zu der Prozessoreinheit 104, 104a, 104b übertragen wird, von welcher die Fehlermeldung anschließend über die Prozessoreinheit-Ausgabemittel 203, 203a, 203b zu einer externen Anzeigeeinheit und/oder einer Fehlerverarbeitungseinheit ausgegeben wird.

Die erfindungsgemäße Rechnervorrichtung kann auch dadurch ausgelegt werden, dass an Stelle der in jeweiligen Prozessoreinheiten 104, 104a, 104b zugeordneten Selbsttesteinheiten 105, 105a, 105b weitere Prozessormodule bereitgestellt werden, welche die Durchführung von Selbsttests bezüglich der jeweiligen Prozessoreinheit 104, 104a, 104b ausführen.

Somit ergibt sich der wesentliche Vorteil, dass neben einem Selbsttest der Prozessoreinheiten ein Vergleich von Anfangswerten, Zwischenwerten bzw. Zwischenergebnissen und Endergebnissen über die Verbindungsmittel 108a bzw. 108b möglich ist.

Weitere Vorteile ergeben sich aus der Kombination des Selbsttestverfahrens aus Prozessoreinheit und Selbsttesteinheit mit dem Dualprozessor aus zwei Prozessoreinheiten:

(i) durch zyklisch ausgeführte Selbsttests können „schlafende" Fehler in durch die Prozessdatenverarbeitung nicht verwendeten Teilen der Prozessoreinheiten aufgedeckt werden, so dass fehlerhafte Prozessoreinheiten stillgelegt werden können, bevor

sich der Fehler durch einen Wertevergleich zwischen den Prozessoren bemerkbar macht;

(ii) der zusätzlich kontinuierlich ausgeführte Austausch und Vergleich von Werten zwischen den Prozessoreinheiten stellt sämtliche akuten Fehler, die sich in einer Wertedifferenz auswirken, mit einer hohen Fehlerabdeckung fest;

(iii) nach einem Auftreten eines durch den Wertevergleich zwischen zwei Prozessoren entdeckten Fehlers wird durch den anschließenden zyklischen Selbsttest die defekte Prozessoreinheit identifiziert und stillgelegt, so dass die funktionsfähige Prozessoreinheit weiterarbeiten kann - diese Vorgehensweise erhöht die Verfügbarkeit der Rechnervorrichtung, da nicht bei jedem akuten Fehler abgeschaltet werden muss.

Obwohl die vorliegende Erfindung vorstehend anhand bevorzugter Ausführungsbeispiele beschrieben wurde, ist sie darauf nicht beschränkt, sondern auf vielfältige Weise modifizierbar.

Auch ist die Erfindung nicht auf die genannten Anwendungsmöglichkeiten beschränkt.

PATENTANSPRÜCHE

1. Rechnervorrichtung (100, 100a, 100b, 100c) für sicherheitskritische Anwendungen, mit:

a) mindestens einer Prozessoreinheit (104; 104a, 104b);

b) einer Speichereinheit (102) zur Speicherung von Prozessdaten;

c) einer Speicherverwaltungseinheit (103) zur Steuerung von Speicherzugriffen in der Rechnervorrichtung (100; 100a, 100b, 100c);

d) einer Fehlererfassungseinheit (101) zur Erfassung von Fehlern in der Speichereinheit (102); und

e) mindestens einer der Prozessoreinheit (104; 104a, 104b) zugeordneten Selbsttesteinheit (105; 105a, 105b),

wobei die Rechnervorrichtung (100, 100a, 100b, 100c) weiter umfasst:

f) Verbindungsmittel (108a, 108b) zur Verbindung der Prozessoreinheiten (104a, 104b) untereinander und mit der Speicherverwaltungseinheit (103), wobei die Prozessoreinheiten (104a, 104b) zusammen mit der Speichereinheit (102) auf einer gemeinsamen Chipfläche angeordnet sind.

2. Vorrichtung nach Anspruch 1,
dadurch gekennzeichnet, dass die Fehlererfassungseinheit (101) als eine Fehlerkorrektureinheit (106) ausgebildet ist, mit welcher eine Korrektur von Fehlern in der Speichereinheit (102) bereitgestellt wird.

3. Vorrichtung nach Anspruch 1,

dadurch gekennzeichnet, dass jeder Prozessoreinheit (104, 104a, 104b) jeweils eine Selbsttesteinheit (105, 105a, 105b) zur Durchführung eines Selbsttests zugeordnet ist.

4. Vorrichtung nach Anspruch 1 und 3,
dadurch gekennzeichnet, dass die Rechnervorrichtung (100) zwei durch Verbindungsmittel (108a, 108b) gekoppelte Prozessoreinheiten (104a, 104b) aufweist, welchen jeweils eine Selbsttesteinheit (105a, 105b) zugeordnet ist.

5. Vorrichtung nach Anspruch 1,
dadurch gekennzeichnet, dass eine Kombination von Rechnervorrichtungen (100a, 100b, 100c), die eine gleiche oder unterschiedliche Anzahl von Prozessoreinheiten (104, 104a, 104b) aufweisen, mittels mindestens einer Verbindungseinheit (107a, 107b) bereitgestellt ist.

6. Vorrichtung nach Anspruch 1 und 2,
dadurch gekennzeichnet, dass in der Rechnervorrichtung (100, 100a, 100b, 100c) jeder Speichereinheit (102) jeweils eine Fehlerkorrektureinheit (106) zugeordnet ist.

7. Vorrichtung nach Anspruch 1,
dadurch gekennzeichnet, dass die Speicherverwaltungseinheit (103) zur Steuerung des Speicherzugriffs in der Rechnervorrichtung (100; 100a, 100b, 100c) und die mindestens eine Prozessoreinheit (104; 104a, 104b) als eine einzige Einheit integral ausgebildet sind.

8. Verfahren zur Prozessdatenverarbeitung in einer Rechnervorrichtung (100, 100a, 100b, 100c) für sicherheitskritische Anwendungen, mit den Schritten:

a) Verarbeiten von Prozessdaten in mindestens einer Prozessoreinheit (104; 104a, 104b), wobei

a1) die mindestens eine Prozessoreinheit (104; 104a, 104b) mittels mindestens einer der Prozessoreinheit (104; 104a, 104b) zugeordneten Selbsttesteinheit (105; 105a, 105b) getestet wird; und

a2) in der Rechnervorrichtung (100, 100a, 100b, 100c) die Prozessoreinheiten (104a, 104b) untereinander und mit der Speicherverwaltungseinheit (103) mittels Verbindungsmitteln (108a, 108b) verbunden sind, wobei die Prozessoreinheiten (104a, 104b) zusammen mit der Speichereinheit (102) auf einer gemeinsamen Chipfläche angeordnet sind;

b) Steuern von Speicherzugriffen in der Rechnervorrichtung (100; 100a, 100b, 100c) mittels einer Speicherverwaltungseinheit (103);

c) Speichern von Prozessdaten in einer Speichereinheit (102); und

d) Erfassen von Fehlern in der Speichereinheit (102) mittels einer Fehlererfassungseinheit (101).

9. Verfahren nach Anspruch 8,
dadurch gekennzeichnet, dass mittels einer Fehlerkorrektureinheit (106) Fehler in der Speichereinheit (102) korrigiert werden.

10. Verfahren nach Anspruch 8,
dadurch gekennzeichnet, dass in der Rechnervorrichtung (100a, 100c) zwei durch Verbindungsmittel (108a, 108b) gekoppelte Prozessoreinheiten (104a, 104b) jeweils durch zugeordnete Selbsttesteinheiten (105a, 105b) getestet werden.

11. Verfahren nach Anspruch 8,
dadurch gekennzeichnet, dass Rechnervorrichtungen (100, 100a, 100b, 100c), die eine gleiche oder unterschiedliche Anzahl von Prozessoreinheiten (104, 104a, 104b) aufweisen, mittels min-

destens einer Verbindungseinheit (107a, 107b) kombiniert werden.

12. Verfahren nach Anspruch 8 und 9,
dadurch gekennzeichnet, dass die Speichereinheit (102) in der Rechnervorrichtung (100, 100a, 100b, 100c) jeweils mittels einer zugeordneten Fehlerkorrektureinheit (106) auf Fehler überprüft und korrigiert wird.

13. Verfahren nach Anspruch 8,
dadurch gekennzeichnet, dass die mindestens eine Prozessoreinheit (104; 104a, 104b) mittels einer zugeordneten Selbsttesteinheit (105; 105a, 105b) getestet wird.

14. Verfahren nach Anspruch 8,
dadurch gekennzeichnet, dass die Selbsttesteinheit (105; 105a, 105b) eine Fehlermeldung über Selbsttesteinheit-Ausgabemittel (202, 202a, 202b) zu einer externen Anzeigeeinheit und/oder einer Fehlerverarbeitungseinheit ausgibt, wenn eine Prozessoreinheit (104, 104a, 104b) durch die zugeordnete Selbsttesteinheit (105; 105a, 105b) als fehlerhaft erkannt wird.

15. Verfahren nach Anspruch 8,
dadurch gekennzeichnet, dass die Prozessoreinheiten (104, 104a, 104b) Anfangswerte, Zwischenergebnisse bzw. Zwischenwerte und Endergebnisse über die Verbindungsmittel (108a, 108b) zwischen den Prozessoreinheiten (104, 104a, 104b) austauschen und auf Gleichheit überprüfen.

16. Verfahren nach Anspruch 15,
dadurch gekennzeichnet, dass die Prozessoreinheit (104, 104a, 104b) eine Fehlermeldung über Prozessoreinheit-Ausgabemittel (203, 203a, 203b) zu einer externen Anzeigeeinheit und/oder einer Fehlerverarbeitungseinheit ausgibt, wenn die Prozessoreinheit (104, 104a, 104b) eine Abweichung zwischen den Zwischenergebnissen bzw. Zwischenwerten und/oder den Endergebnissen feststellt.

17. Verfahren nach Anspruch 8,
dadurch gekennzeichnet, dass bei einem Auftreten von Fehlern in der Speichereinheit (102) eine Fehlermeldung über Fehlererfassungseinheit-Ausgabemittel (204) zu einer externen Anzeigeeinheit und/oder einer Fehlerverarbeitungseinheit ausgegeben wird.

18. Verfahren nach Anspruch 8,
dadurch gekennzeichnet, dass bei einem Auftreten von Fehlern in der Speichereinheit (102) eine Fehlermeldung über die Speicherverwaltungseinheit (103) zu der Prozessoreinheit (104, 104a, 104b) übertragen wird, von welcher die Fehlermeldung anschließend über die Prozessoreinheit-Ausgabemittel (203, 203a, 203b) zu einer externen Anzeigeeinheit und/oder einer Fehlerverarbeitungseinheit ausgegeben wird.

ZUSAMMENFASSUNG

Vorrichtung für sicherheitskritische Anwendungen und sichere Elektronik-Architektur

Die Erfindung schafft eine Rechnervorrichtung für sicherheitskritische Anwendungen mit mindestens einer Prozessoreinheit, und mindestens einer einer Prozessoreinheit zugeordneten Selbsttesteinheit (105, 105a, 105b), einer Speichereinheit (102) zur Speicherung des Programms und von Prozessdaten, einer Speicherverwaltungseinheit (103) zur Steuerung von Speicherzugriffen in der Rechnervorrichtung, einer Fehlererfassungseinheit (101) zur Erfassung von Fehlern in der Speichereinheit (102), wobei Verbindungsmittel zur Verbindung der Prozessoreinheiten untereinander und mit der Speicherverwaltungseinheit (103) vorgesehen sind, wobei die Prozessoreinheiten zusammen mit der Speichereinheit auf einer gemeinsamen Chipfläche angeordnet sind.

Figur 3

FIG 1

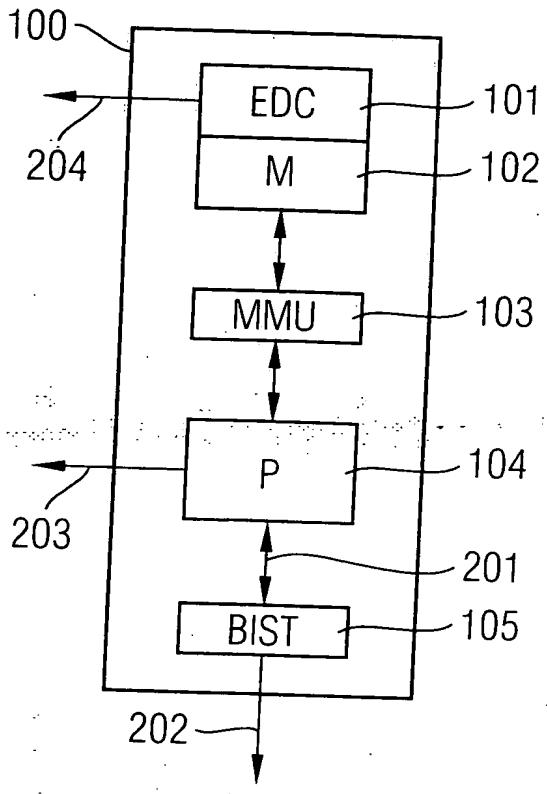

100
EDC
101
204
M
102
MMU
103
P
104
203
201
BIST
105
202

FIG 2

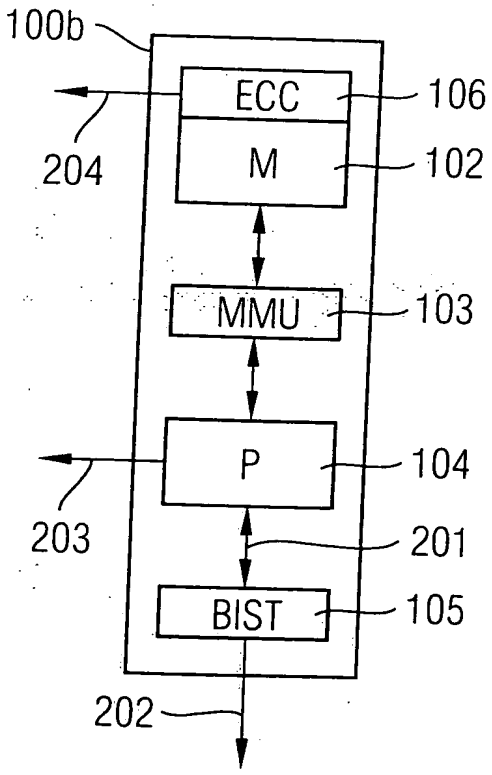

100b
ECC
106
204
M
102
MMU
103
P
104
203
201
BIST
105
202

FIG 3

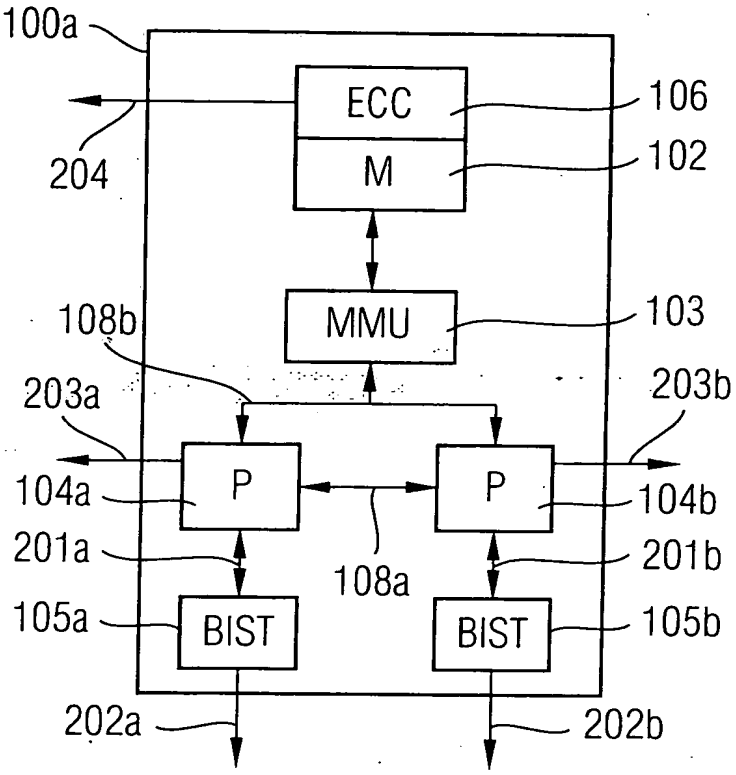

100a
ECC
106
204
M
102
MMU
103
108b
203a
203b
P
P
104a
104b
201a
201b
108a
105a
BIST
BIST
105b
202a
202b

FIG 4

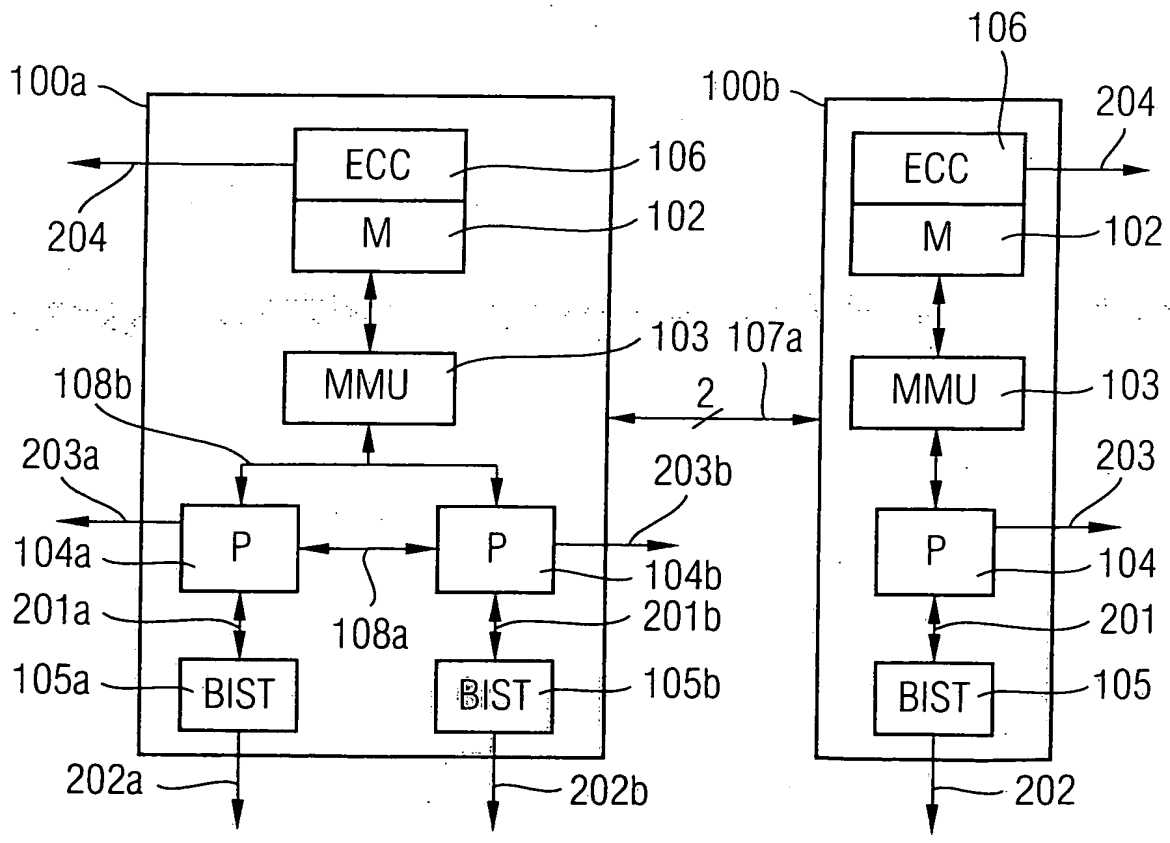
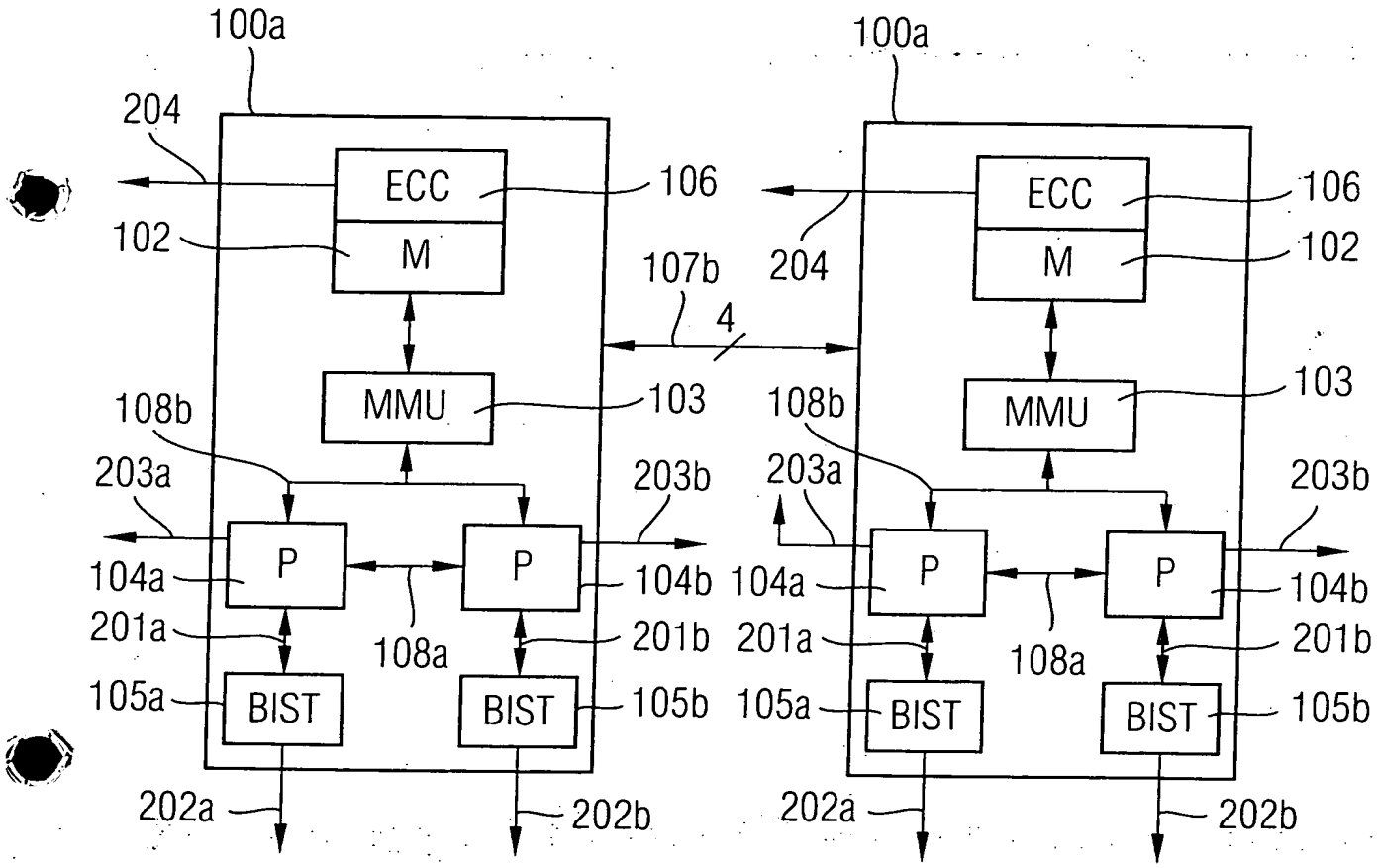

106
100a
100b
204
ECC
ECC
106
204
M
M
102
102
103
107a
MMU
MMU
103
108b
2
203a
203b
203
P
P
P
104a
104b
104
201a
108a
201b
201
105a
BIST
BIST
BIST
105b
105
202a
202b
202

FIG 5


100a
204
ECC
106
102
M
107b
4
MMU
103
108b
203a
203b
P
P
104a
104b
201a
108a
201b
105a
BIST
BIST
105b
202a
202b
100a
204
ECC
106
M
102
MMU
103
108b
203a
203b
P
P
104a
104b
201a
108a
201b
105a
BIST
BIST
105b
202a
202b